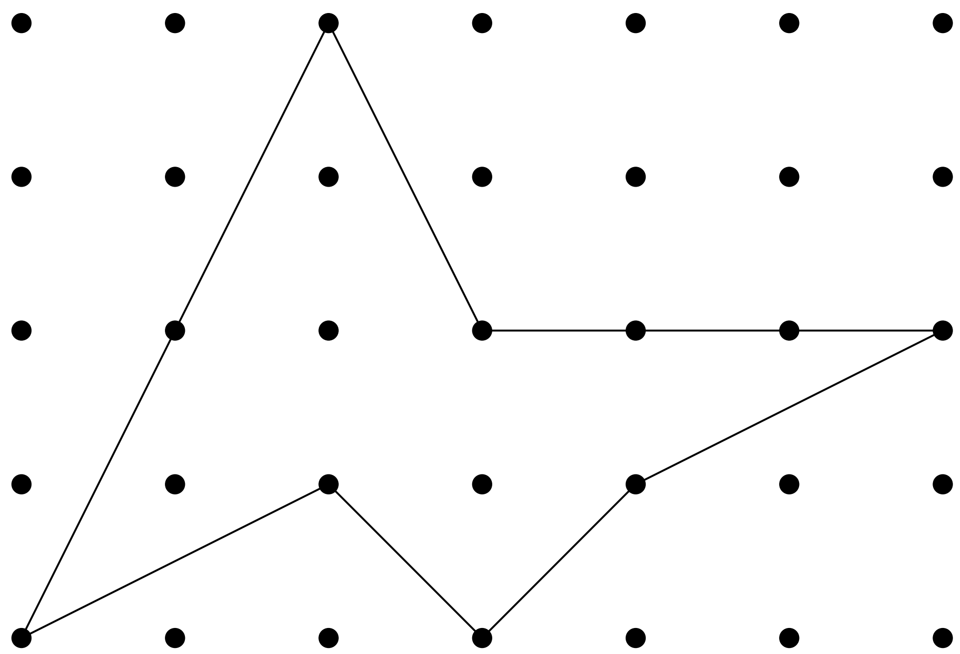
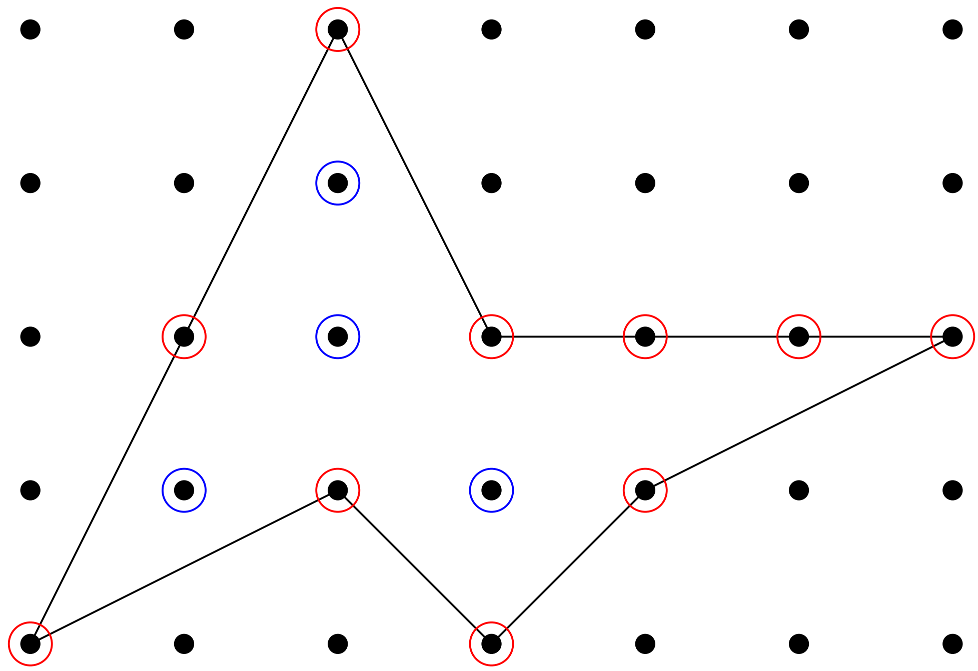
Georg Alexander Pick (1859–1942)

P: lattice polygon in $\mathbb{R}^2$
(vertices $\in \mathbb{Z}^2$, no self-intersections)





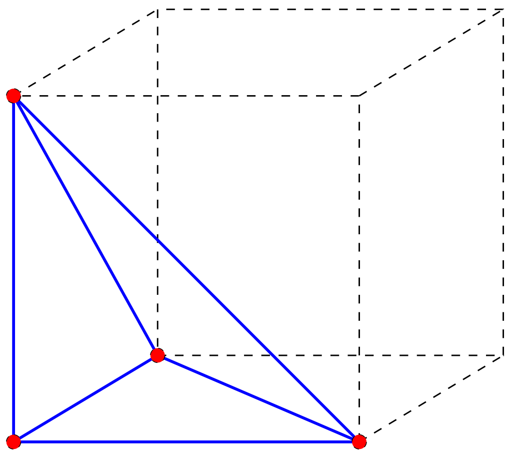
$$\mathbf{A} = \text{area of } P$$
$$\mathbf{I} = \#\text{ interior points of } P (= 4)$$
$$\mathbf{B} = \#\text{boundary points of } P (= 10)$$

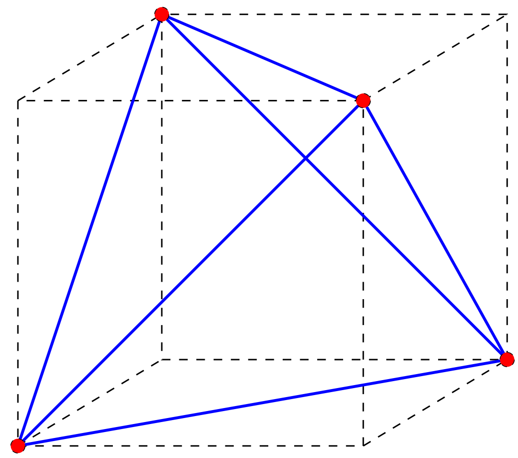
Then

$$\mathbf{A} = \frac{2\mathbf{I} + \mathbf{B} - 2}{2} = \frac{2 \cdot \mathbf{4} + \mathbf{10} - 2}{2} = 9.$$

Pick's theorem (seemingly) fails in higher dimensions. For example, let T_1 and T_2 be the tetrahedra with vertices

$$v(T_1) = \{(0,0,0),(1,0,0),(0,1,0),(0,0,1)\}$$
$$v(T_2) = \{(0,0,0),(1,1,0),(1,0,1),(0,1,1)\}.$$





Then

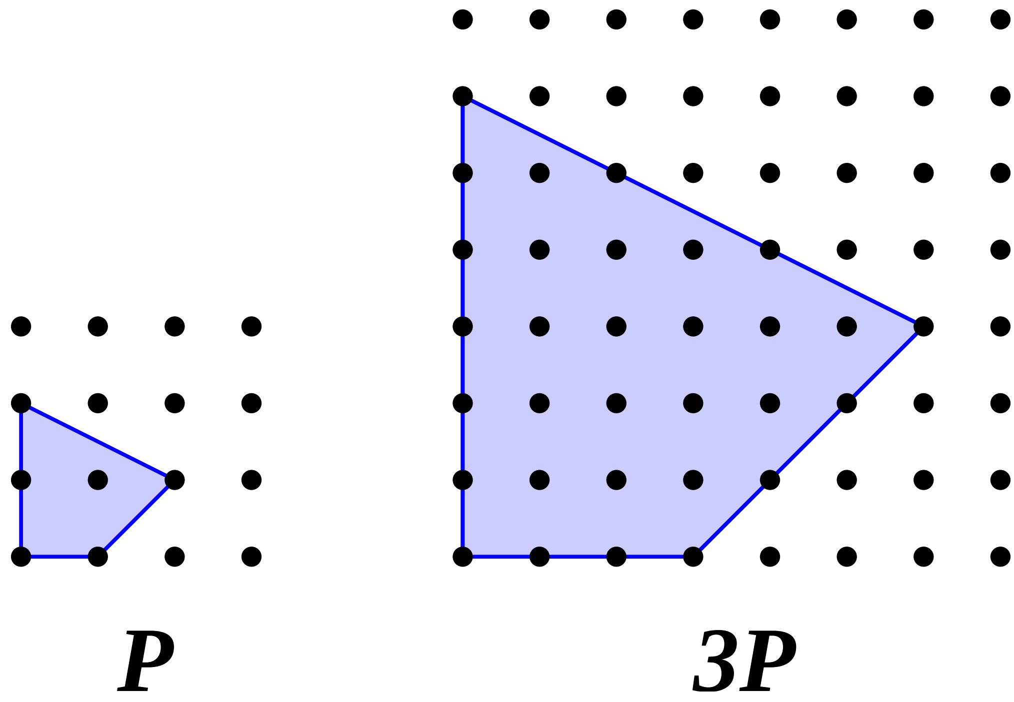
$$I(T_1) = I(T_2) = 0$$

$$B(T_1) = B(T_2) = 4$$

$$A(T_1) = 1/6, \quad A(T_2) = 1/3.$$

Let $\mathcal{P}$ be a convex polytope (convex hull of a finite set of points) in $\mathbb{R}^d$. For $n \geq 1$, let

$$n\mathcal{P} = \{n\alpha : \alpha \in \mathcal{P}\}.$$



Let

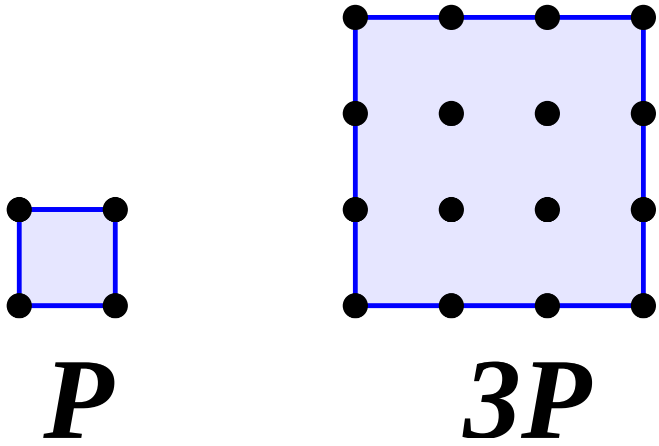
$$\begin{aligned} \boldsymbol{i(\mathcal{P}, n)} &= \#(n\mathcal{P} \cap \mathbb{Z}^d) \\ &= \#\{\alpha \in \mathcal{P} \,:\, n\alpha \in \mathbb{Z}^d\}, \end{aligned}$$

the number of lattice points in $n\mathcal{P}$.

Similarly let

$$\boldsymbol{\mathcal{P}^\circ} = \text{interior of } \mathcal{P} = \mathcal{P} - \partial\mathcal{P}$$

$$\begin{aligned} \boldsymbol{\bar{i}(\mathcal{P}, n)} &= \#(n\mathcal{P}^\circ \cap \mathbb{Z}^d) \\ &= \#\{\alpha \in \mathcal{P}^\circ \,:\, n\alpha \in \mathbb{Z}^d\}, \end{aligned}$$



$$i(\mathcal{P}, n) = (n+1)^2$$

$$\bar{i}(\mathcal{P}, n) = (n-1)^2 = i(\mathcal{P}, -n).$$

lattice polytope: polytope with integer vertices

Theorem (Reeve, 1957). *Let* $\mathcal{P}$ *be a three-dimensional lattice polytope. Then the volume* $V(\mathcal{P})$ *is a certain (explicit) function of* $i(\mathcal{P},1)$, $\bar{i}(\mathcal{P},1)$, *and* $i(\mathcal{P},2)$.

Theorem (Ehrhart 1962, Macdonald 1963) *Let*

$\mathcal{P}$ = lattice polytope in $\mathbb{R}^N$, $\dim \mathcal{P} = d$.

*Then $i(\mathcal{P}, n)$ is a polynomial (the **Ehrhart polynomial** of $\mathcal{P}$) in n of degree d. Moreover,*

$$\begin{aligned} i(\mathcal{P}, 0) &= 1 \\ \bar{i}(\mathcal{P}, n) &= (-1)^d i(\mathcal{P}, -n),\ n > 0 \end{aligned}$$

(reciprocity).

If $d = N$ then

$i(\mathcal{P}, n) = V(\mathcal{P})n^d +$ lower order terms,

where $\boldsymbol{V(\mathcal{P})}$ *is the volume of $\mathcal{P}$.*

Corollary (generalized Pick's theorem). *Let* $\mathcal{P} \subset \mathbb{R}^d$ *and* $\dim \mathcal{P} = d$. *Knowing any* d *of* $i(\mathcal{P}, n)$ *or* $\bar{i}(\mathcal{P}, n)$ *for* $n > 0$ *determines* $V(\mathcal{P})$.

Proof. Together with $i(\mathcal{P}, 0) = 1$, this data determines $d+1$ values of the polynomial $i(\mathcal{P}, n)$ of degree d. This uniquely determines $i(\mathcal{P}, n)$ and hence its leading coefficient $V(\mathcal{P})$. $\square$

Example. When $d = 3$, $V(\mathcal{P})$ is determined by

$$\begin{aligned} i(\mathcal{P}, 1) &= \#(\mathcal{P} \cap \mathbb{Z}^3) \\ i(\mathcal{P}, 2) &= \#(2\mathcal{P} \cap \mathbb{Z}^3) \\ \bar{i}(\mathcal{P}, 1) &= \#(\mathcal{P}^\circ \cap \mathbb{Z}^3), \end{aligned}$$

which gives Reeve's theorem.

Example (magic squares). Let $\mathcal{B}_M \subset \mathbb{R}^{M\times M}$ be the **Birkhoff polytope** of all $M \times M$ **doubly-stochastic** matrices $A = (a_{ij})$, i.e.,

$$a_{ij} \geq 0$$

$$\sum_i a_{ij} = 1 \text{ (column sums 1)}$$

$$\sum_j a_{ij} = 1 \text{ (row sums 1).}$$

Note. $B = (b_{ij}) \in n\mathcal{B}_M \cap \mathbb{Z}^{M \times M}$ if and only if

$$b_{ij} \in \mathbb{N} = \{0, 1, 2, \ldots\}$$

$$\sum_i b_{ij} = n$$

$$\sum_j b_{ij} = n.$$

$$\begin{bmatrix} 2 & 1 & 0 & 4 \\ 3 & 1 & 1 & 2 \\ 1 & 3 & 2 & 1 \\ 1 & 2 & 4 & 0 \end{bmatrix} \qquad (M = 4,\ n = 7)$$

$$\boldsymbol{H_M(n)} := \#\{M \times M \ \mathbb{N}\text{-matrices, line sums } n\} = i(\mathcal{B}_M, n).$$

E.g.,

$$H_1(n) = 1$$
$$H_2(n) = n + 1$$

$$\begin{bmatrix} a & n-a \\ n-a & a \end{bmatrix}, \quad 0 \leq a \leq n.$$

$$H_3(n) = \binom{n+2}{4} + \binom{n+3}{4} + \binom{n+4}{4}$$

(MacMahon)

$$H_M(0) = 1$$
$$H_M(1) = M! \text{ (permutation matrices)}$$

Theorem (Birkhoff-von Neumann) *The vertices of $\mathcal{B}_M$ consist of the $M!$ $M \times M$ permutation matrices. Hence $\mathcal{B}_M$ is a lattice polytope.*

Corollary (Anand-Dumir-Gupta conjecture) *$H_M(n)$ is a polynomial in n (of degree $(M-1)^2$).*

Example. $H_4(n) = \frac{1}{11340}\Big(11n^9$

$$+198n^8 + 1596n^7 + 7560n^6 + 23289n^5$$
$$+48762n^5 + 70234n^4 + 68220n^2$$
$$+40950n + 11340\Big).$$

Reciprocity $\Rightarrow$

$$\pm H_M(-n) = \#\{M \times M \text{ matrices } B \text{ of } \textbf{positive} \text{ integers, line sum } n\}.$$

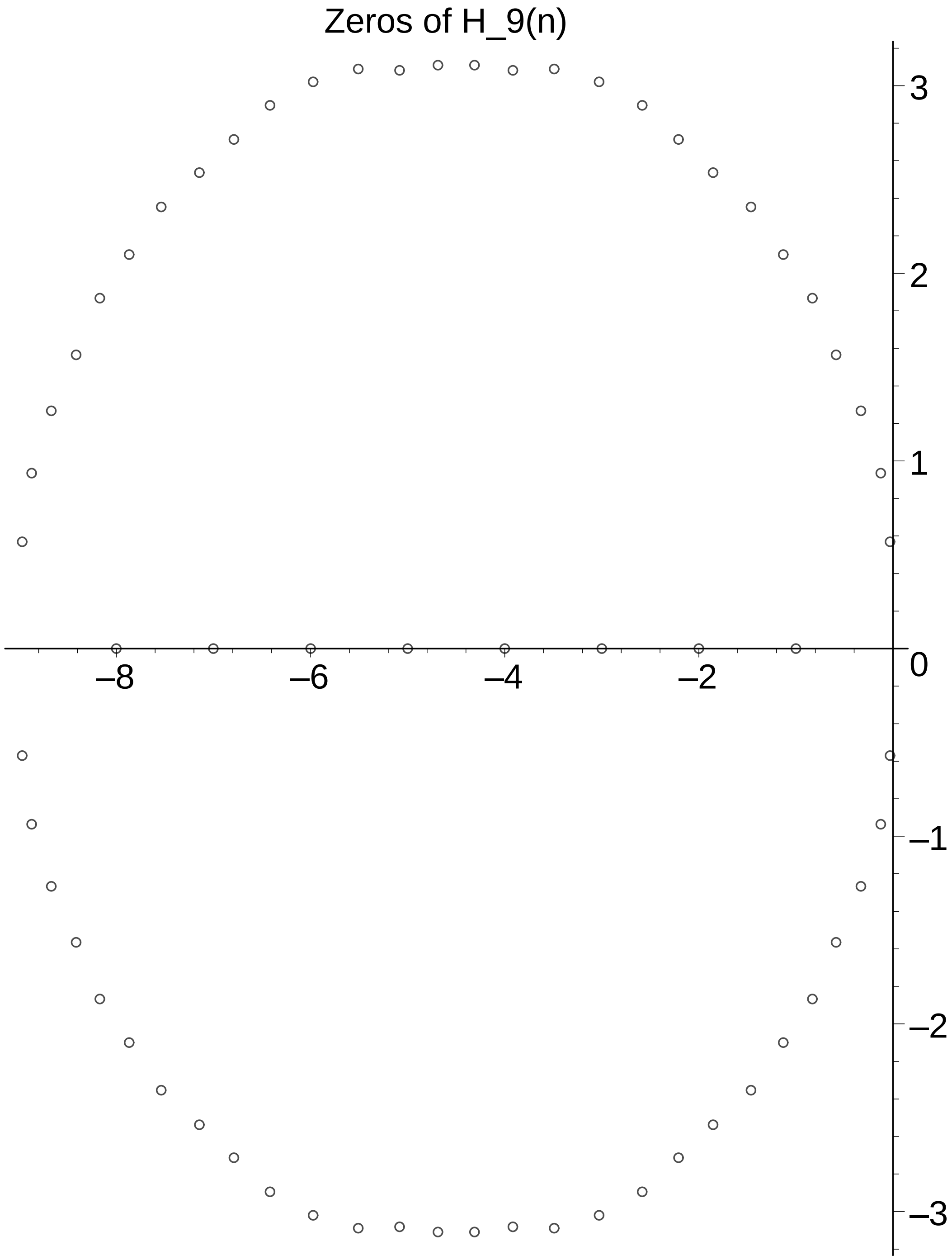
But every such B can be obtained from an $M \times M$ matrix A of **nonnegative** integers by adding 1 to each entry.

Corollary. $H_M(-1) = H_M(-2) = \cdots = H_M(-M+1) = 0$

$$H_M(-M-n) = (-1)^{M-1} H_M(n)$$

(greatly reduces computation)

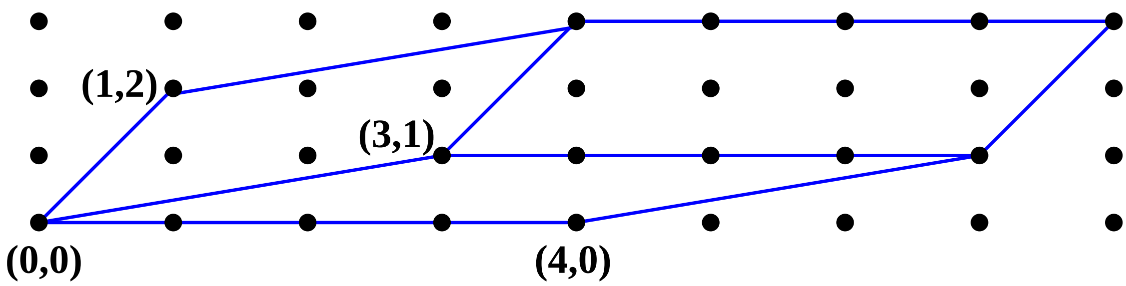
Applications e.g. to statistics (contingency tables).


Zeros of H_9(n)
3
2
1
0
–1
–2
–3
–8
–6
–4
–2

Zonotopes. Let $v_1, \ldots, v_k \in \mathbb{R}^d$. The **zonotope** $Z(v_1, \ldots, v_k)$ generated by $v_1, \ldots, v_k$:

$$Z(v_1, \ldots, v_k) = \{\lambda_1 v_1 + \cdots + \lambda_k v_k \ :\ 0 \leq \lambda_i \leq 1\}$$

Example. $v_1 = (4,0)$, $v_2 = (3,1)$, $v_3 = (1,2)$



Theorem. *Let*

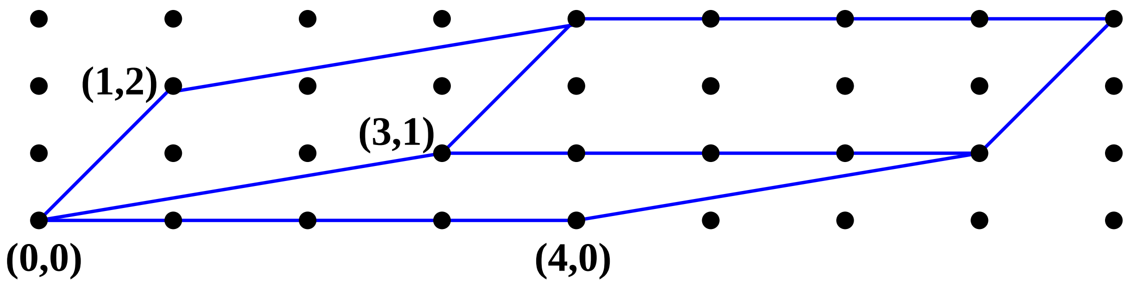
$$Z = Z(v_1, \ldots, v_k) \subset \mathbb{R}^d,$$

where $v_i \in \mathbb{Z}^d$*. Then*

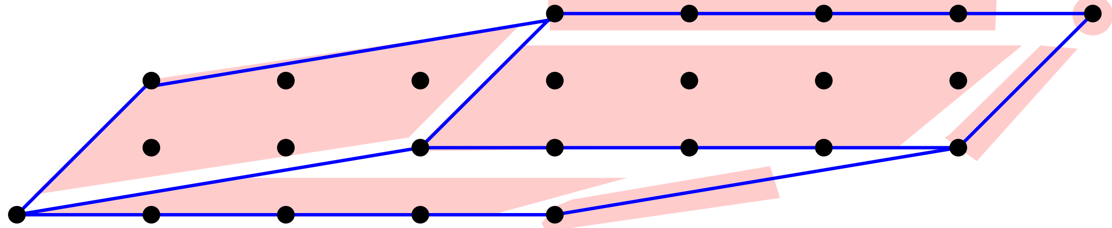
$$i(Z, 1) = \sum_X h(X),$$

where X *ranges over all linearly independent subsets of* $\{v_1, \ldots, v_k\}$*, and* $h(X)$ *is the gcd of all* $j \times j$ *minors (*$j = \#X$*) of the matrix whose rows are the elements of* X*.*

Example. $v_1 = (4,0)$, $v_2 = (3,1)$, $v_3 = (1,2)$



$$\begin{aligned} i(Z,1) &= \begin{vmatrix} 4 & 0 \\ 3 & 1 \end{vmatrix} + \begin{vmatrix} 4 & 0 \\ 1 & 2 \end{vmatrix} + \begin{vmatrix} 3 & 1 \\ 1 & 2 \end{vmatrix} \\ &\quad + \gcd(4,0) + \gcd(3,1) \\ &\quad + \gcd(1,2) + \det(\emptyset) \\ &= 4+8+5+4+1+1+1 \\ &= 24. \end{aligned}$$



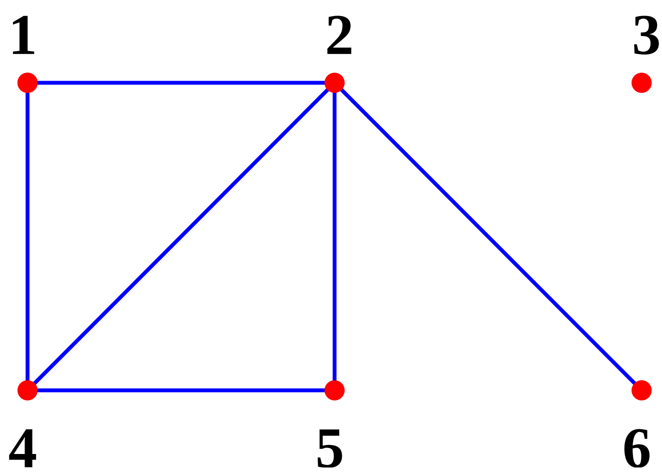
Let $\boldsymbol{G}$ be a graph (with no loops or multiple edges) on the vertex set $\boldsymbol{V(G)} = \{1, 2, \ldots, n\}$. Let

$\boldsymbol{d_i}$ = degree (# incident edges) of vertex i.

Define the **ordered degree sequence** $\boldsymbol{d(G)}$ of G by

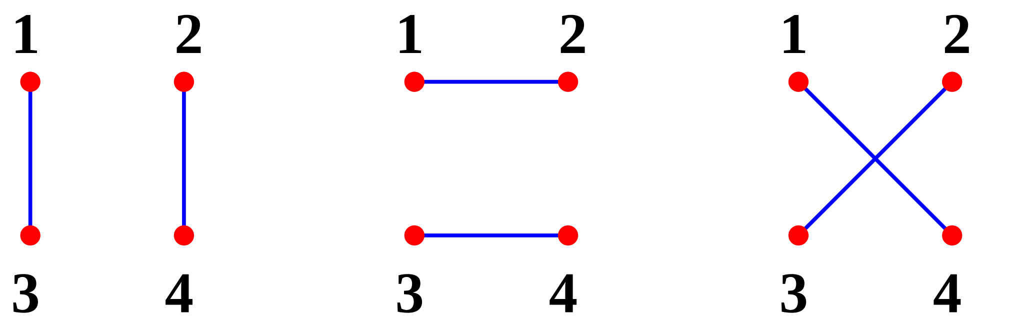
$$d(G) = (d_1, \ldots, d_n).$$

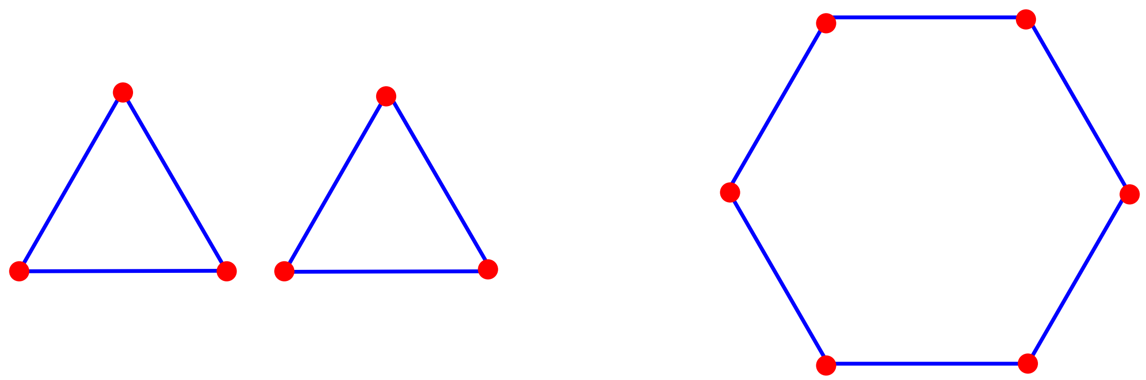
Example. $d(G) = (2, 4, 0, 3, 2, 1)$



Let $\boldsymbol{f(n)}$ be the number of distinct $d(G)$, where $V(G) = \{1, 2, \ldots, n\}$.

Example. If $n \leq 3$, all $d(G)$ are distinct, so $f(1) = 1$, $f(2) = 2^1 = 2$, $f(3) = 2^3 = 8$. For $n \geq 4$ we can have $G \neq H$ but $d(G) = d(H)$, e.g.,





In fact, $f(4) = 54 < 2^6 = 64$.

Let **conv** denote convex hull, and

$\boldsymbol{\mathcal{D}_n} = \mathrm{conv}\{d(G) : V(G) = \{1, \ldots, n\}\}$,

the **polytope of degree sequences** (Perles, Koren).

Easy fact. Let $\boldsymbol{e_i}$ be the ith unit coordinate vector in $\mathbb{R}^n$. E.g., if $n = 5$ then $e_2 = (0, 1, 0, 0, 0)$. Then

$$\mathcal{D}_n = Z(e_i + e_j : 1 \le i < j \le n).$$

Theorem (Erdős-Gallai). *Let* $\boldsymbol{\alpha} = (a_1, \ldots, a_n) \in \mathbb{Z}^n$. *Then* $\alpha = d(G)$ *for some* G *if and only if*

- $\alpha \in \mathcal{D}_n$
- $a_1 + a_2 + \cdots + a_n$ *is even.*

"Fiddling around" leads to:

Theorem. *Let*

$$F(x) = \sum_{n\geq 0} f(n)\frac{x^n}{n!}$$
$$= 1 + x + 2\frac{x^2}{2!} + 8\frac{x^3}{3!} + 54\frac{x^4}{4!} + \cdots .$$

Then

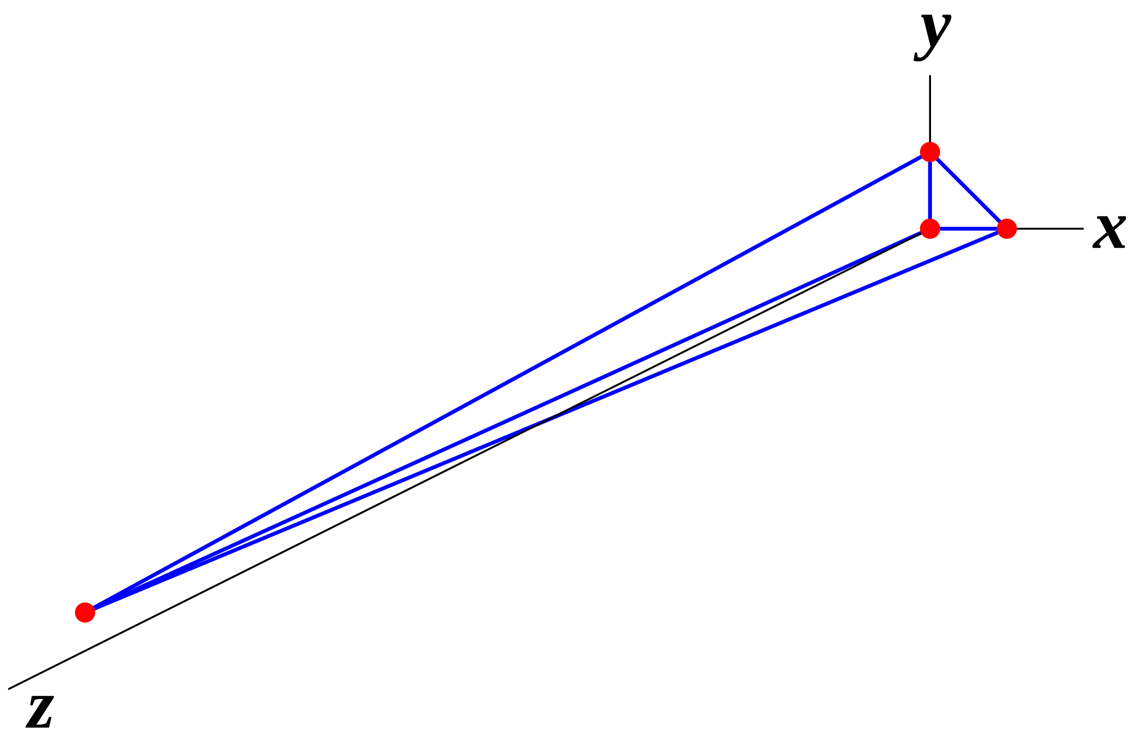
$$F(x) = \frac{1}{2}\left[\left(1 + 2\sum_{n\geq 1} n^n \frac{x^n}{n!}\right)^{1/2} \times \left(1 - \sum_{n\geq 1}(n-1)^{n-1}\frac{x^n}{n!}\right) + 1\right] \times \exp \sum_{n\geq 1} n^{n-2}\frac{x^n}{n!}.$$

The h-vector of $i(\mathcal{P}, n)$

Let $\mathcal{P}$ denote the tetrahedron with vertices $(0,0,0)$, $(1,0,0)$, $(0,1,0)$, $(1,1,13)$. Then

$$i(\mathcal{P}, n) = \frac{13}{6}n^3 + n^2 - \frac{1}{6}n + 1.$$

Thus in general the coefficients of Ehrhart polynomials are not "nice." Is there a "better" basis?


y
x
z

Let $\mathcal{P}$ be a lattice polytope of dimension d. Since $i(\mathcal{P}, n)$ is a polynomial of degree d, $\exists\ h_i \in \mathbb{Z}$ such that

$$\sum_{n \geq 0} i(\mathcal{P}, n) x^n = \frac{h_0 + h_1 x + \cdots + h_d x^d}{(1-x)^{d+1}}.$$

Definition. Define

$$\boldsymbol{h}(\mathcal{P}) = (h_0, h_1, \ldots, h_d),$$

the ***h*-vector** of $\mathcal{P}$.

Example. Recall

$$i(\mathcal{B}_4, n) = \frac{1}{11340}(11n^9$$
$$+198n^8 + 1596n^7 + 7560n^6 + 23289n^5$$
$$+48762n^5 + 70234n^4 + 68220n^2$$
$$+40950n + 11340).$$

Then

$$h(\mathcal{B}_4) = (1, 14, 87, 148, 87, 14, 1, 0, 0, 0).$$

Elementary properties of $h(\mathcal{P}) = (h_0, \ldots, h_d)$:

- $h_0 = 1$
- $h_d = (-1)^{\dim \mathcal{P}} i(\mathcal{P}, -1) = I(\mathcal{P})$
- $\max\{i : h_i \neq 0\} = \min\{j \geq 0 : i(\mathcal{P}, -1) = i(\mathcal{P}, -2) = \cdots$
$$= i(\mathcal{P}, -(d-j)) = 0\}$$
E.g., $h(\mathcal{P}) = (h_0, \ldots, h_{d-2}, 0, 0) \Leftrightarrow i(\mathcal{P}, -1) = i(\mathcal{P}, -2) = 0$.
- $i(\mathcal{P}, -n-k) = (-1)^d i(\mathcal{P}, n)\ \forall n \Leftrightarrow$
$$h_i = h_{d+1-k-i}\ \forall i, \text{and}$$
$$h_{d+2-k-i} = h_{d+3-k-i} = \cdots = h_d = 0$$

Recall:

$$h(\mathcal{B}_4) = (1, 14, 87, 148, 87, 14, 1, 0, 0, 0).$$

Thus

$$i(\mathcal{B}_4, -1) = i(\mathcal{B}_4, -2) = i(\mathcal{B}_4, -3) = 0$$

$$i(\mathcal{B}_4, -n-4) = -i(\mathcal{B}_4, n).$$

Theorem A (nonnegativity). (McMullen, RS) $h_i \geq 0$.

Theorem B (monotonicity). (RS) *If $\mathcal{P}$ and $\mathcal{Q}$ are lattice polytopes and $\mathcal{Q} \subseteq \mathcal{P}$, then $h_i(\mathcal{Q}) \leq h_i(\mathcal{P})$ $\forall i$.*

B $\Rightarrow$ A: take $\mathcal{Q} = \emptyset$.

Theorem A can be proved geometrically, but Theorem B requires **commutative algebra**.

$$\mathcal{P} = \text{lattice polytope in } \mathbb{R}^d$$

$\boldsymbol{R} = \boldsymbol{R_{\mathcal{P}}}$ = vector space over K with basis $\{x^\alpha y^n : \alpha \in \mathbb{Z}^d,\ n \in \mathbb{P},\ \alpha/n \in \mathcal{P}\} \cup \{1\}$, where if $\alpha = (\alpha_1, \ldots, \alpha_d)$ then

$$\boldsymbol{x^\alpha} = x_1^{\alpha_1} \cdots x_d^{\alpha_d}.$$

If $\alpha/m, \beta/n \in \mathcal{P}$, then

$$(\alpha + \beta)/(m + n) \in \mathcal{P}$$

by convexity. Hence $R_{\mathcal{P}}$ is a **subalgebra** of the polynomial ring $K[x_1, \ldots, x_d, y]$.

Example. (a) Let

$$\mathcal{P} = \operatorname{conv}\{(0,0),(0,1),(1,0),(1,1)\}.$$

Then

$$R_{\mathcal{P}} = K[y, x_1\, y, x_2\, y, x_1 x_2\, y].$$

(b) Let

$$\mathcal{P} = \operatorname{conv}\{(0,0,0),(1,1,0),(1,0,1),(0,1,1)\}.$$

Then

$$R_{\mathcal{P}} = K[y, x_1 x_2\, y, x_1 x_3\, y, x_2 x_3\, y, x_1 x_2 x_3\, y^2].$$

Let

$$\boldsymbol{R_n} = \mathrm{span}_K\{x^\alpha y^n \ : \ \alpha/n \in \mathcal{P}\},$$

with $\boldsymbol{R_0} = \mathrm{span}_K\{1\} = K$. Then

$$R = R_0 \oplus R_1 \oplus \cdots \quad \text{(vector space } \oplus\text{)}$$

$$R_i R_j \subseteq R_{i+j}.$$

Thus R is a **graded algebra**. Moreover,

$$\begin{aligned} \dim_K R_n &= \#\{x^\alpha y^n \ : \ \alpha/n \in \mathcal{P}\} \\ &= i(\mathcal{P}, n). \end{aligned}$$

Thus $i(\mathcal{P}, n)$ is the **Hilbert function** of R. Moreover,

$$F(\mathcal{P}, x) := \sum_{n \geq 0} i(\mathcal{P}, n) x^n$$

is the **Hilbert series** of $R_{\mathcal{P}}$.

Theorem (Hochster). *Let $\mathcal{P}$ be a lattice polytope of dimension d. Then $R_{\mathcal{P}}$ is a* ***Cohen-Macaulay*** *ring.*

This means: $\exists$ algebraically independent $\theta_1, \ldots, \theta_{d+1} \in R_1$ (called a **homogeneous system of parameters** or **h.s.o.p.**) such that $R_{\mathcal{P}}$ is a finitely generated free module over

$$S = K[\theta_1, \ldots, \theta_{d+1}].$$

Thus $\exists\ \eta_1, \ldots, \eta_s$ ($\eta_i \in R_{e_i}$) such that

$$R_{\mathcal{P}} = \bigoplus_{i=1}^{s} \eta_i S$$

and $\eta_i S \cong S$ (as S-modules).

Now

$$\begin{aligned} F(R_{\mathcal{P}}, x) &:= \sum_{n \geq 0} i(\mathcal{P}, n) x^n \\ &= \sum_{i=1}^{s} x^{e_i} F(S, x) \\ &= \frac{\sum_{i=1}^{s} x^{e_i}}{(1-x)^{d+1}}. \end{aligned}$$

Compare with

$$F(R_{\mathcal{P}}, x) = \frac{h_0 + h_1 x + \cdots + h_d x^d}{(1-x)^{d+1}}$$

to conclude:

Corollary. $\sum_{i=1}^{s} x^{e_i} = \sum_{j=0}^{d} h_j x^j$. *In particular,* $h_i \geq 0$.

Now suppose:

$\boldsymbol{\mathcal{P}}$, $\boldsymbol{\mathcal{Q}}$: lattice polytopes in $\mathbb{R}^N$

$$\dim \mathcal{P} = \boldsymbol{d}, \quad \dim \mathcal{Q} = \boldsymbol{e}$$

$$\mathcal{Q} \subseteq \mathcal{P}.$$

Let

$$\boldsymbol{I} = \mathrm{span}_K\{x^\alpha y^n \ : \ \alpha \in \mathbb{Z}^N,\ \alpha/n \in \mathcal{P} - \mathcal{Q}\}.$$

Easy: I is an ideal of $R_{\mathcal{P}}$ and

$$R_{\mathcal{P}}/I \cong R_{\mathcal{Q}}.$$

Lemma. $\exists$ *an h.s.o.p.* $\theta_1, \ldots, \theta_{d+1}$ *for* $R_{\mathcal{P}}$ *such that* $\theta_1, \ldots, \theta_{e+1}$ *is an h.s.o.p. for* $R_{\mathcal{Q}}$ *and*

$$\theta_{e+2}, \ldots, \theta_{d+1} \in I.$$

Thus

$$R_{\mathcal{Q}}/(\theta_1, \ldots, \theta_{e+1}) \cong R_{\mathcal{Q}}/(\theta_1, \ldots, \theta_{d+1}),$$

so the natural surjection $\boldsymbol{f} : R_{\mathcal{P}} \to R_{\mathcal{Q}}$ induces a (degree-preserving) surjection

$$\bar{\boldsymbol{f}} : A_{\mathcal{P}} := R_{\mathcal{P}}/(\theta_1, \ldots, \theta_{d+1})$$
$$\to A_{\mathcal{Q}} := R_{\mathcal{Q}}/(\theta_1, \ldots, \theta_{e+1}).$$

Since $R_{\mathcal{P}}$ and $R_{\mathcal{Q}}$ are Cohen-Macaulay,

$\dim(A_{\mathcal{P}})_i = h_i(\mathcal{P})$, $\dim(A_{\mathcal{Q}})_i = h_i(\mathcal{Q})$.

The surjection

$$(A_{\mathcal{P}})_i \to (A_{\mathcal{Q}})_i$$

gives $h_i(\mathcal{P}) \geq h_i(\mathcal{Q})$. $\square$

Zeros of Ehrhart polynomials.

Sample theorem (de Loera, Develin, Pfeifle, RS) *Let $\mathcal{P}$ be a lattice d-polytope. Then*

$$i(\mathcal{P}, \alpha) = 0,\ \alpha \in \mathbb{R} \Rightarrow -d \leq \alpha \leq \lfloor d/2 \rfloor.$$

Theorem. *Let d be odd. There exists a 0/1 d-polytope $\mathcal{P}_d$ and a real zero α_d of $i(\mathcal{P}_d, n)$ such that*

$$\lim_{\substack{d\to\infty \\ d \text{ odd}}} \frac{\alpha_d}{d} = \frac{1}{2\pi e} = 0.0585\cdots.$$

Open. Is the set of all complex zeros of all Ehrhart polynomials of lattice polytopes dense in $\mathbb{C}$? (True for chromatic polynomials of graphs.)

Further directions

- $R_{\mathcal{P}}$ is the coordinate ring of a projective algebraic variety $X_{\mathcal{P}}$, a **toric variety**. Leads to deep connections with toric geometry, including new formulas for $i(\mathcal{P}, n)$.
- **Complexity.** Computing $i(\mathcal{P}, n)$, or even $i(\mathcal{P}, 1)$ is **#*P*-complete**. Thus an "efficient" (polynomial time) algorithm is extremely unlikely. However:

  Theorem (A. Barvinok, 1994). *For* ***fixed*** $\dim \mathcal{P}$, *∃ polynomial-time algorithm for computing* $i(\mathcal{P}, n)$.

Reference. M. Barvinok and J. Pommersheim, An algorithmic theory of lattice points in polyhedra, in *New Perspectives in Algebraic Combinatorics*, MSRI Publications, vol. 38, 1999, pp. 91–147.